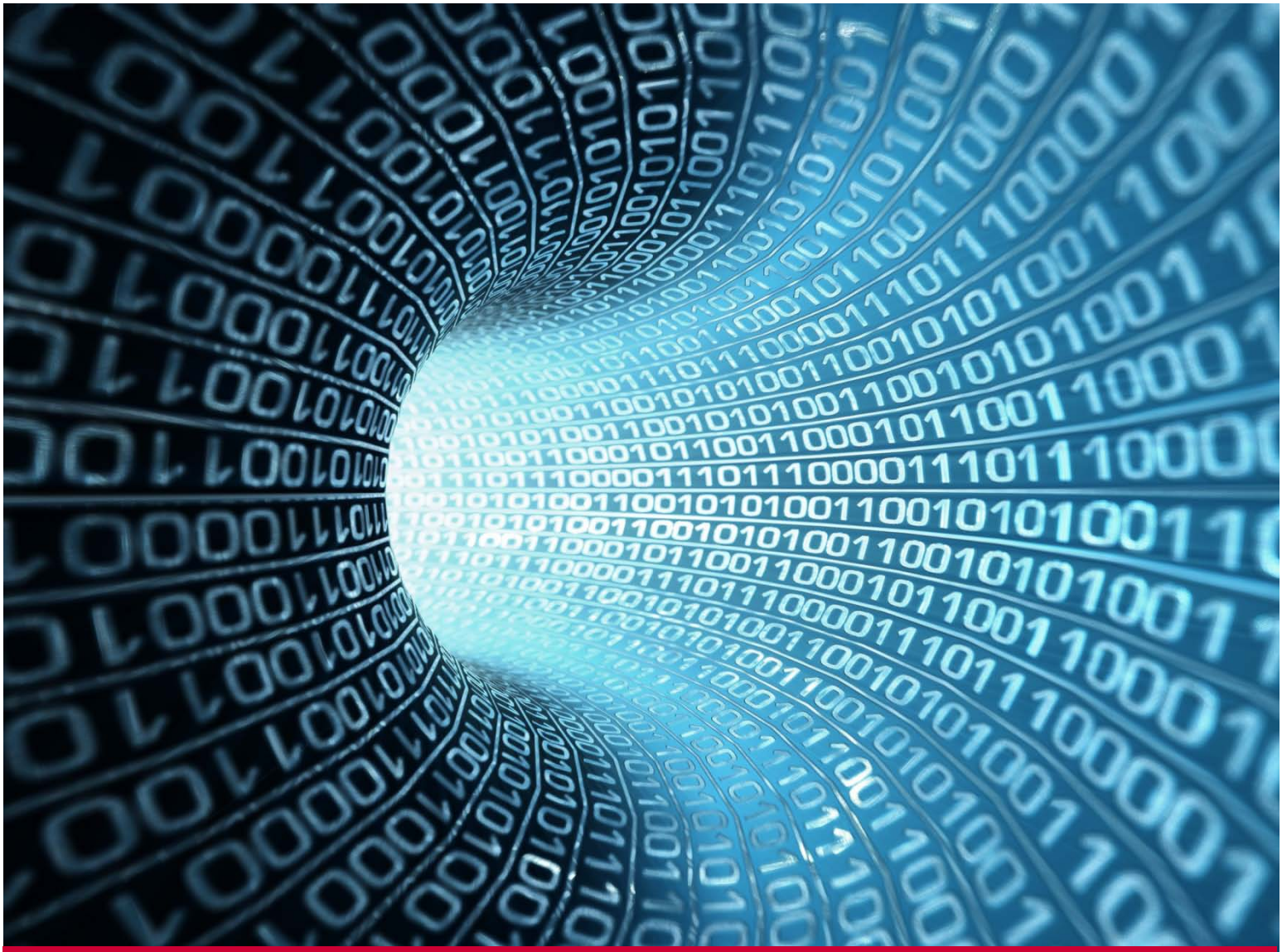

DHS Privacy Office

2010 Data Mining Report to Congress

December 2010

Homeland Security

Foreword

I am pleased to present the Department of Homeland Security's (DHS) 2010 Data Mining Report to Congress. Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53, entitled the Federal Agency Data Mining Reporting Act of 2007, requires DHS to report annually to the Congress on DHS activities that meet the Act's definition of data mining. For each identified activity, the Act requires DHS to provide (1) a thorough description of the activity; (2) the technology and methodology used; (3) the sources of data used; (4) an analysis of the activity's efficacy; (5) the legal authorities supporting the activity; and (5) an analysis of the activity's impact on privacy and the protections in place to protect privacy. This is the fifth comprehensive DHS Data Mining Report, and the third report prepared pursuant to the Act.

When it created DHS, the Congress authorized the Department to engage in data mining and other analytical tools in furtherance of Departmental goals and objectives. Consistent with the rigorous compliance process applied to all DHS programs and systems, the DHS Privacy Office has worked closely with the programs discussed in this report to ensure that they employ data mining in a manner that both supports the Department's mission to protect the homeland and protects privacy.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable Joseph R. Biden
President, United States Senate

The Honorable Christopher S. Bond
Vice Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Susan M. Collins
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable John Conyers, Jr.
Chairman, U.S. House of Representatives Committee on the Judiciary

The Honorable Dianne Feinstein
Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Peter Hoekstra
Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable Darrell Issa
Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Peter T. King
Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Patrick J. Leahy
Chairman, U.S. Senate Committee on the Judiciary

The Honorable Joseph I. Lieberman
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Nancy Pelosi
Speaker, U.S. House of Representatives

The Honorable Silvestre Reyes
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable Lamar Smith
Ranking Member, U.S. House of Representatives Committee on the Judiciary

The Honorable Jeff Sessions
Ranking Member, U.S. Senate Committee on the Judiciary

The Honorable Bennie G. Thompson
Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Edolphus Towns
Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

Inquiries relating to this report may be directed to the DHS Office of Legislative Affairs at 202-447-5890.

Sincerely,

Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security

Executive Summary

The Department of Homeland Security Privacy Office (DHS Privacy Office or Office) is providing this report to the Congress pursuant to the Department's obligations under section 804 of the Implementing the Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), entitled the Federal Agency Data Mining Reporting Act of 2007 (Data Mining Reporting Act or the Act).[1] This report discusses activities currently deployed or under development in the Department that meet the Data Mining Reporting Act's definition of data mining, and provides the information set out in the Act's reporting requirements for data mining activities.[2]

In the 2009 DHS Data Mining Report,[3] the DHS Privacy Office identified three DHS programs that engage in activities that meet the Data Mining Reporting Act's definition of data mining: (1) the Automated Targeting System (ATS) Inbound, Outbound, and Passenger modules administered by U.S. Customs and Border Protection (CBP); (2) the Data Analysis and Research for Trade Transparency System (DARTTS) administered by U.S. Immigration and Customs Enforcement (ICE); and (3) the Freight Assessment System (FAS) administered by the Transportation Security Administration (TSA). This year's report, covering the time period from December 2009 through November 2010, includes complete descriptions of each of these programs, with updates on modifications, additions, or other developments that have occurred since the 2009 DHS Data Mining Report was issued. After consulting with the DHS components, the DHS Privacy Office identified no additional DHS activities during the current reporting year that meet the Act's definition of data mining.

The Homeland Security Act of 2002, as amended (Homeland Security Act), expressly authorizes the Department to use data mining, among other analytical tools, in furtherance of its mission.[4] DHS exercises this authority to engage in data mining in the programs discussed in this report, all of which have been reviewed by the DHS Chief Privacy Officer for potential impact on privacy. The Chief Privacy Officer's authority for reviewing DHS data mining activities stems from three principal sources: the Privacy Act of 1974, as amended (Privacy Act);[5] the E-Government Act of 2002 (E-Government Act);[6] and section 222 of the Homeland Security Act, which states, in part, that the Chief Privacy Officer is responsible for "assuring that the [Department's] use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information."[7]

The DHS Privacy Office's privacy compliance policies and procedures are based on a set of eight Fair Information Practice Principles (FIPPs) that are rooted in the tenets of the Privacy Act and memorialized in *Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*.[8]

[1] 42 U.S.C. § 2000ee-3.
[2] The Act's definition of data mining is discussed below on page 5, and the Act's reporting requirements are included in Appendix A.
[3] http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2009_12.pdf.
[4] 6 U.S.C. § 121(d)(14).
[5] 5 U.S.C. § 552a.
[6] Pub. L. No. 107-347.
[7] 6 U.S.C. § 142(a)(1).
[8] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

The DHS Privacy Office applies the FIPPs to the full breadth and diversity of information and interactions within DHS, including DHS activities that involve data mining.

As described more fully below, the DHS Privacy Office's compliance process requires programs using Personally Identifiable Information (PII) to complete federally-mandated privacy documentation, consisting of a Privacy Impact Assessment (PIA), as required by the E-Government Act,[9] and a System of Records Notice (SORN), as required by the Privacy Act.[10] The DHS Privacy Office has worked closely with the programs discussed in this report to complete the required privacy compliance documentation. The programs that use PII in connection with their data mining activities – ATS and DARTTS – have issued both PIAs and SORNs.

While each of the programs described below engages to some extent in data mining, none uses data mining to make unevaluated automated decisions about individuals. These programs do not make decisions about individuals solely on the basis of data mining results. In all cases, DHS employees conduct investigations to verify (or disprove) the results of data mining, and then bring their own judgment and experience to bear in making determinations about individuals initially identified through data mining activities. The DHS Privacy Office continues to work closely with each of these programs to ensure that their required privacy compliance documentation is current and that privacy protections have been implemented.

[9] Pub. L. No. 107-347.
[10] 5 U.S.C. § 552a(e)(4).

Table of Contents

I. Background

A. DHS Privacy Office Authorities

The Department of Homeland Security Privacy Office (DHS Privacy Office or Office) is the first statutorily mandated privacy office in the federal government. Its mission is to preserve and enhance privacy protections for all individuals, to promote transparency of DHS operations, and to serve as a leader in the privacy community. The Office works to minimize the impact of DHS programs on an individual's privacy, particularly an individual's personal information and dignity, while achieving the Department's mission to protect the homeland. The Chief Privacy Officer reports directly to the Secretary of the Department, and the Office's mission and authority are founded upon the responsibilities set forth in the Homeland Security Act of 2002, as amended (Homeland Security Act).[11]

The DHS Privacy Office serves as the steward of section 222 of the Homeland Security Act. The Office also ensures that the Department complies with the Privacy Act, the Freedom of Information Act (FOIA),[12] the E-Government Act, and the numerous laws, Executive Orders, court decisions, and Departmental policies that protect the collection, use, and disclosure of personal and Departmental information. The Privacy Act embodies a code of fair information principles that govern the collection, maintenance, use, and dissemination of personally identifiable information (PII) by federal agencies. The E-Government Act mandates Privacy Impact Assessments (PIAs) for all federal agencies when there are new collections of, or new technologies applied to, PII. FOIA codifies the right of access to records in the possession and control of federal agencies, subject to certain limited exemptions and law enforcement exclusions.

The Chief Privacy Officer is also the Department's Chief FOIA Officer, and the DHS Privacy Office's operations reflect these dual roles. The Office manages and formulates the above statutory and policy-based responsibilities in a collaborative environment with DHS component privacy officers or Privacy Points of Contact (PPOC)[13] and program offices to ensure that all privacy issues receive the appropriate level of review and expertise. In addition, the DHS Privacy Office assures Department-wide statutory compliance with FOIA and the Privacy Act, as well as the consistent handling of disclosure requests pursuant to both Acts.

[11] 6 U.S.C. § 142. The authorities and responsibilities of the Chief Privacy Officer were last amended by the 9/11 Commission Act on August 3, 2007. The 9/11 Commission Act added investigatory authority, the power to issue subpoenas, and the ability to administer oaths, affirmations, or affidavits necessary to investigate or report on matters relating to responsibilities under section 222 of the Homeland Security Act. These responsibilities are further described on the DHS Privacy Office website (http://www.dhs.gov/privacy) and in the *DHS Privacy Office 2010 Annual Report to Congress available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2010.pdf .

[12] 5 U.S.C. § 552.

[13] Component privacy officers are senior-level DHS employees who are responsible for privacy within their respective components. All operational components of DHS have privacy officers. PPOCs assume the duties of component privacy officers in other components that do not have full-time privacy officers. The network of component privacy officers and PPOCs works closely with component program managers and the DHS Privacy Office to manage privacy matters within DHS.

B. Data Mining and the DHS Privacy Compliance Process

This is the DHS Privacy Office's fifth comprehensive report to Congress on DHS activities that involve data mining, and the third report pursuant to the Data Mining Reporting Act.[14] The Homeland Security Act expressly authorizes the Department to use data mining, among other analytical tools, in furtherance of its mission.[15] DHS exercises this authority to engage in data mining in the programs discussed in this report, all of which have been reviewed by the Chief Privacy Officer for potential impacts on privacy. The DHS Chief Privacy Officer's authority for reviewing DHS data mining activities stems from three principal sources: the Privacy Act, the E-Government Act, and the Homeland Security Act, which states, in part, that the DHS Chief Privacy Officer is responsible for "assuring that the [Department's] use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information."[16] The DHS Privacy Office compliance process discussed below is designed to identify and mitigate risks to privacy that may be posed by any DHS program, project, or information technology system.

The DHS Privacy Office's privacy compliance policies and procedures are based on the Fair Information Practice Principles (FIPPs), which are rooted in the tenets of the Privacy Act and memorialized in the December 2008 *Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*.[17] The FIPPs govern the appropriate use of PII at the Department. DHS uses the FIPPs to enhance privacy protections by assessing the nature and purpose of all PII collected to ensure it fulfills the Department's mission to preserve, protect, and secure the homeland. Thus, the DHS Privacy Office applies the FIPPs to the full breadth and diversity of information and interactions within DHS, including DHS activities that involve data mining.

DHS uses three main documents related to privacy compliance: (1) the Privacy Threshold Analysis (PTA); (2) the PIA; and (3) the System of Record Notice (SORN). While each of these documents has a distinct function in implementing privacy policy at DHS, together these documents further the transparency of Department activities and demonstrate accountability.

- **PTAs:** The PTA is the first document completed by a DHS component seeking to implement or modify a system, program, technology, project, or rulemaking. The PTA identifies whether the system, program, technology, or project is privacy sensitive and thus requires additional privacy compliance documentation such as a PIA or SORN.
- **PIAs:** PIAs are an important tool for examining the privacy impact of IT systems, programs, technologies, projects, or rule-makings. The PIA is the method by which the DHS Privacy Office's Compliance Group reviews system management activities in key areas such as

[14] All of the DHS Privacy Office's Data Mining Reports are available on the DHS Privacy Office web site at http://www.dhs.gov/privacy.
[15] The Act states that, "[s]ubject to the direction and control of the Secretary, the responsibilities of the Under Secretary for Information Analysis and Infrastructure Protection, shall be as follows . . . To establish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including data mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate." 6 U.S.C. § 121(d)(13).
[16] 6 U.S.C. § 142(a)(1).
[17] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

security and how information is collected, used, and shared. If a PIA is required, the DHS component will draft the PIA for review by the component privacy officer or PPOC and component counsel. Part of the PIA analysis includes determining whether an existing SORN appropriately covers the activity or a new SORN is required. Once the PIA is approved at the component level, the component privacy officer or PPOC submits it to the DHS Privacy Office Compliance Group for review and approval by the Chief Privacy Officer.

- **SORNs:** SORNs provide notice to the public regarding Privacy Act information collected by a system of records, as well as insight into how information is used, retained, and may be corrected. Part of the Privacy Act analysis requires determining whether certain Privacy Act exemptions should be taken to protect the records from disclosure to an individual because of law enforcement or national security reasons. If a SORN is required, the program manager will work with the component privacy officer or PPOC and component counsel to write a SORN and submit it to the DHS Privacy Office compliance group for review and approval by the Chief Privacy Officer.

PTAs, PIAs, and SORNs serve the common purpose of identifying and documenting areas of privacy focus for programs, IT systems, and collections of PII.[18]

The DHS Privacy Office identifies DHS programs that engage in data mining through several different processes. The DHS Privacy Office reviews all OMB-300 budget submissions to learn of programs or systems that use PII and to determine whether they address privacy appropriately.[19] The DHS Privacy Office uses the PTA to review all information technology systems that are going through the certification and accreditation (C&A) process required under the Federal Information Security Management Act of 2002 (FISMA)[20] to determine whether they maintain PII. The PIA process also provides the DHS Privacy Office insight into technologies used or intended to be used by DHS. In addition, the DHS Privacy Office reviews technology investment proposals that the DHS Enterprise Architecture Center of Excellence and Integrated Project Teams process, to ensure that DHS investments in technology include a specific review for compliance with privacy protection requirements. All of these oversight activities provide the DHS Privacy Office opportunities to learn about proposed data mining activities and to engage program managers in discussions about potential privacy issues.

The Privacy Office has worked closely with the relevant DHS components to complete the privacy compliance documentation required for each of the programs described in this Report.

[18] Once the PTA, PIA, and SORN are completed, the documents are periodically scheduled for a mandatory review by the DHS Privacy Office (timing varies by document type). For systems that require only PTAs and PIAs, the review process begins again three years after the document is complete or when there is an update to the program, whichever comes first. The process begins with either the update or submission of a new PTA. The Privacy Act requires that SORNs be reviewed on a biennial basis.

[19] All major DHS IT programs are reviewed by the DHS Privacy Office Compliance Group on an annual basis, prior to submission to OMB for inclusion in the President's annual budget. The Compliance Group plays a substantial role in the review of the OMB budget submissions (known as Exhibit 300s) prior to submission to OMB. *See* Office of Mgmt. & Budget, Executive Office of the President, OMB Circular No. A-11, Section 300, *Planning, Budgeting, Acquisition, and Management of Capital Assets*, *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s300.pdf.

[20] Title 44, U.S.C., Chapter 35, Subchapter III (Information Security).

As discussed more fully below, a PTA has been completed for all of these programs; programs that use PII have issued both PIAs and SORNs.

C. Federal Agency Data Mining Reporting Act Requirements

The Data Mining Reporting Act defines "data mining" as:

> *a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where—*
>
> *(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;*
>
> *(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and*
>
> *(C) the purpose of the queries, searches, or other analyses is not solely—*
>
> *(i) the detection of fraud, waste, or abuse in a Government agency or program;*
>
> *or*
>
> *(ii) the security of a Government computer system.*[21]

The Act expressly excludes queries, searches, or analyses that are conducted solely in electronic databases of publicly-available information: telephone directories, news reporting services, databases of legal and administrative rulings, and other databases and services providing public information without a fee.[22]

Two aspects of the Act's definition of "data mining" are worth emphasizing. First, the definition is limited to *pattern-based* electronic searches, queries or analyses. Activities that use only PII or other terms specific to individuals (e.g., a license plate number), as search terms are excluded from the definition. Second, the definition is limited to searches, queries or analyses that are conducted for the purpose of identifying predictive patterns or anomalies that are indicative of terrorist or criminal activity by an individual or individuals. Research in electronic databases that produces only a summary of historical trends, therefore, is not "data mining" under the Act.

The Act requires the Department to provide the Congress a detailed description of each DHS activity that meets the Act's definition of "data mining," including the methodology and technology used, the sources of the data being analyzed, the legal authority for the activity, a discussion of the activity's efficacy in achieving its purpose, and an analysis of the activity's impact on privacy and the policies and procedures in place to protect the privacy and due process rights of individuals.[23] The DHS Privacy Office addresses these reporting requirements for each of the DHS programs included in this Report.

[21] 42 U.S.C. § 2000ee-3(b)(1).
[22] 42 U.S.C. § 2000ee-3(b)(2).
[23] 42 U.S.C. § 2000ee-3(c)(2).

II. Reporting

In the 2008 DHS Data Mining Report,[24] the DHS Privacy Office identified three Department programs that engage in data mining as defined by the Data Mining Reporting Act: (1) the Automated Targeting System (ATS) Cargo Inbound, Cargo Outbound, and Passenger modules, which are administered by U.S. Customs and Border Protection (CBP); (2) the Data Analysis and Research for Trade Transparency System (DARTTS), which is administered by U.S. Immigration and Customs Enforcement (ICE); and (3) the Freight Assessment System (FAS), which is administered by the Transportation Security Administration (TSA). The 2009 DHS Data Mining Report[25] provided updated descriptions of these programs based on program changes occurring in the 2009 reporting year. This year's report presents the complete descriptions of these programs provided in the 2008 and 2009 DHS Data Mining Reports, with updates on modifications, additions, or other developments that have occurred in the current reporting year. As was the case in 2009, the DHS Privacy Office identified no additional DHS data mining activities during the current reporting year.

A. Automated Targeting System (ATS)

1. 2010 Program Update

During the current reporting period CBP added the Report of International Transportation of Currency or Monetary Instruments Form (CMIR)[26] as a new data source for the ATS Passenger module (ATS-P). CBP improved auditing and user tracking capabilities within ATS-P, in an effort to improve its control over the use of Passenger Name Record (PNR) data and its ability to audit said use. These internal improvements enhanced CBP's and DHS' abilities to report on their compliance with the Agreement between the European Union and the United States of America on the processing and transfer of PNR data. Separately, CBP began development of a new module in ATS, the Intelligence and Operations Framework System (IOFS), to provide workflow, case management, and collaboration with respect to targeting and analytical findings across CBP disciplines. The functionality of IOFS permits search results, data analyses, and text documents to be displayed for further editing, development, and storage as a working document.

2. General Program Description

CBP developed ATS, an intranet-based enforcement and decision support tool that is the cornerstone for all CBP targeting efforts. ATS compares traveler, cargo, and conveyance information against intelligence and other enforcement data by incorporating risk-based targeting scenarios and assessments. CBP uses ATS to improve the collection, use, analysis, and dissemination of information that is gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the United States. CBP also uses ATS to identify other violations of U.S. laws that CBP enforces. In this way, ATS allows CBP officers charged with enforcing U.S. law and preventing terrorism and other crimes to focus their efforts on travelers, conveyances, and cargo shipments that most warrant greater scrutiny. ATS standardizes names, addresses, conveyance names, and similar data so these data

[24] http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_200812.pdf.
[25] http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2009_12.pdf.
[26] The CMIR is the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) Form 105.

elements can be more easily associated with other business data and personal information to form a more complete picture of a traveler, import, or export in context with previous behavior of the parties involved. Traveler, conveyance, and shipment data are processed through ATS and are subject to a real-time, rules-based evaluation.

ATS consists of six modules that focus on exports, imports, passengers and crew (airline passengers and crew on international flights, and passengers and crew on sea carriers), private vehicles crossing at land borders, and import trends over time. This report discusses three of these modules: ATS-Inbound and ATS-Outbound (both of which involve the analysis of cargo), and ATS-P (which involves analysis of information about certain travelers, as discussed below). The remaining modules do not involve data mining as defined by the Data Mining Reporting Act.[27]

Additionally, CBP is developing IOFS, a new module for ATS. IOFS is a platform for temporary and permanent storage of data that is being developed into an analytical product that may be permanently stored as a case within IOFS or in another system. IOFS permits review and cross referencing of analytical products and data from several different systems. IOFS permits CBP to relate information from several ATS modules (specifically ATS-P and ATS-Inbound) and portions of other CBP and federal agency systems (e.g., enforcement case tracking, Border Patrol Significant Incident Reports, and the Department of State's Consolidated Consular Database (CCD), and the Passport Information Electronic Records System (PIERS) to support case development and collaboration between field and headquarters analytical staffs. IOFS supports the work of both Office of Field Operations officers and border patrol agents at the ports of entry, in the field, and in the National Targeting Centers.

A legacy organization of CBP, the U.S. Customs Service traditionally employed computerized screening tools to target potentially high-risk cargo entering, exiting, and transiting the United States. ATS was originally designed as a rules-based program to identify such cargo; it did not apply to travelers. ATS-Inbound and ATS-Outbound became operational in 1997. ATS-P became operational in 1999 and is now critically important to CBP's mission. ATS-P allows CBP officers to determine whether a variety of potential risk indicators exist for travelers and/or their itineraries that may warrant additional scrutiny. ATS-P maintains PNR data, which is data provided to airlines and travel agents by or on behalf of air passengers seeking to book travel. CBP began receiving PNR data voluntarily from certain air carriers in 1997. Currently, CBP collects this information to the extent collected by carriers in connection with a flight into or out of the United States, as part of its border enforcement mission and pursuant to the Aviation and Transportation Security Act of 2001 (ATSA).[28]

ATS receives various data in real time from the following CBP mainframe systems: the Automated Commercial System (ACS), the Automated Manifest System (AMS), the DHS Advance Passenger Information System (APIS), the Automated Export System (AES), the Automated Commercial Environment (ACE), the DHS Electronic System for Travel Authorization (ESTA), the DHS Nonimmigrant Information System (NIIS), DHS Border

[27] These other modules are: ATS-Land (which provides targeting capability for private vehicles arriving by land); ATS-Trend Analysis and Analytical Selectivity Program (ATS-TAP) (which provides trend analysis of historical international trade statistics to identify anomalous activity in aggregate); and ATS-International, which is being developed to support collaborative efforts with foreign customs administrations.

[28] 49 U.S.C. § 44909. The regulations implementing ATSA are codified at 19 C.F.R. § 122.49d.

Crossing Information (BCI), and TECS. TECS includes information from the Federal Bureau of Investigation (FBI) Terrorist Screening Center's (TSC)[29] Terrorist Screening Database (TSDB) and other government databases regarding individuals with outstanding wants and warrants and other high-risk individuals and entities. ATS collects PNR data directly from air carriers. ATS also collects data from certain express consignment services in ATS-Inbound. ATS accesses data from these sources, which collectively include: electronically filed bills of lading, entries, and entry summaries for cargo imports; shippers' export declarations and transportation bookings and bills for cargo exports; manifests for arriving and departing passengers; land-border crossing and referral records for vehicles crossing the border; airline reservation data; nonimmigrant entry records; records from secondary referrals, incident logs, suspect and violator indices; seizures; and information from the TSDB and other government databases regarding individuals with outstanding wants and warrants and other high-risk entities. Finally, ATS uses data from Dun & Bradstreet, a commercially available data source, to assist with company identification through name and address matching.

In addition to providing a risk-based assessment system, ATS provides a graphical user interface for many of the underlying legacy systems from which ATS pulls information. This interface improves the user experience by providing the same functionality in a more rigidly controlled access environment than the underlying system. Access to this functionality of ATS uses existing technical security and privacy safeguards associated with the underlying systems.

A large number of rules are included in the ATS modules that encapsulate sophisticated concepts of business activity that help identify suspicious or unusual behavior. The ATS rules are constantly evolving to both meet new threats and refine existing rules. When evaluating risk, ATS applies the same methodology to all individuals to preclude any possibility of disparate treatment of individuals or groups.

a) ATS-Inbound and ATS-Outbound Modules (Cargo Analytics)

i. Program Description

ATS-Inbound assists CBP officers in identifying inbound cargo shipments that pose a high risk of containing weapons of mass effect, illegal narcotics, or other contraband, and in selecting that cargo for intensive examination. ATS-Inbound is available to CBP officers at all major ports (i.e., air, land, sea, and rail) throughout the United States, and also assists CBP personnel in the Container Security Initiative (CSI) and Secure Freight Initiative (SFI) decision-making processes.

ATS-Outbound aids CBP officers in identifying exports that pose a high risk of containing goods requiring specific export licenses, illegal narcotics, smuggled currency, stolen vehicles or other contraband, or exports that may otherwise be in violation of U.S. law. ATS-Outbound sorts Electronic Export Information (EEI) (formerly referred to as the Shippers' Export Declaration

[29] The TSC is an entity established by the Attorney General in coordination with the Secretary of State, the Secretary of Homeland Security, the Director of the Central Intelligence Agency, the Secretary of the Treasury, and the Secretary of Defense. The Attorney General, acting through the Director of the FBI, established the TSC in support of Homeland Security Presidential Directive 6 (HSPD-6), dated September 16, 2003, which required the Attorney General to establish an organization to consolidate the Federal Government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes. The TSC maintains the Federal Government's consolidated terrorist watch list, known as the TSDB.

(SED)) data extracted from AES, compares it to a set of rules, and evaluates it in a comprehensive fashion. This information assists CBP officers in targeting and/or identifying exports that pose potential aviation safety and security risks (e.g., hazardous materials) or may be otherwise exported in violation of U.S. law.

ATS-Inbound and ATS-Outbound look at data related to cargo in real time and engage in data mining to provide decision support analysis for targeting of cargo for suspicious activity. The cargo analysis provided by ATS is intended to add automated anomaly detection to CBP's existing targeting capabilities, to enhance screening of cargo prior to its entry into the United States.

ii. Technology and Methodology

ATS-Inbound and ATS-Outbound do not collect information directly from individuals. The data used in the development, testing, and operation of ATS-Inbound and ATS-Outbound screening technology is taken from bills of lading and shipping manifest data provided by vendors to CBP as part of the existing cargo screening process. The results of queries, searches, and analyses conducted in the ATS-Inbound and ATS-Outbound system are used to identify anomalous business behavior, data inconsistencies, abnormal business patterns, and suspicious business activity generally. No decisions about individuals are made solely on the basis of these results.

The Security and Accountability for Every Port Act of 2006 (SAFE Port Act) requires ATS to use or investigate the use of advanced algorithms in support of its mission.[30] To that end, ATS has established an Advanced Targeting Initiative, which includes plans for development of data mining, machine learning,[31] and other analytic techniques during the period from FY09 to FY12, for use in ATS-Inbound and ATS-Outbound. Development will take place in iterative phases as the databases to be used by this initiative are updated. The various iterations will be deployed to a select user population, which will test the new functionality. The Advanced Targeting Initiative is being undertaken in tandem with ATS' maintenance and operation of the ATS-Inbound and ATS-Outbound systems. As discussed in the 2009 DHS Data Mining Report, the design and tool-selection processes for data mining, pattern recognition, and machine learning techniques in development in the Advanced Targeting Initiative are under consideration and have yet to be finalized.

iii. Data Sources

As noted above, ATS-Inbound and ATS-Outbound do not collect information directly from individuals. The information maintained in ATS is either collected from private entities providing data in accordance with U.S. legal requirements (e.g., sea, rail and air manifests) or is created by ATS as part of its risk assessments and associated rules.

ATS-Inbound and ATS-Outbound use the information in ATS source databases to gather information about importers and exporters, cargo, and conveyances used to facilitate the importation of cargo into and the exportation of cargo out of the United States. This information includes PII concerning individuals associated with imported and exported cargo (e.g., brokers,

[30] Pub. L. No. 109-347 (2006).

[31] Machine learning is concerned with the design and development of algorithms and techniques that allow computers to "learn." The major focus of machine learning research is to extract information from data automatically, using computational and statistical methods. This extracted information may then be generalized into rules and patterns.

carriers, shippers, buyers, sellers, exporters, freight forwarders, and crew). ATS-Inbound receives data pertaining to entries and manifests from ACS and ACE, and processes it against a variety of rules to make a rapid, automated assessment of the risk of each import.[32] ATS-Outbound uses EEI data that exporters file electronically with AES, export manifest data from AES, export airway bills of lading, and census export data from the U.S. Department of Commerce to assist in formulating risk assessments for cargo bound for destinations outside the United States.

CBP uses commercial off-the-shelf (COTS) software tools to graphically present entity-related information that may represent terrorist or criminal activity, to discover non-obvious relationships across cargo data, to retrieve information from ATS source systems to expose unknown or anomalous activity, and to conduct statistical modeling of cargo-related activities as another approach to detecting anomalous behavior. CBP also uses custom-designed software to resolve ambiguities in trade entity identification related to inbound and outbound cargo.

iv. Efficacy

Based upon the results of testing and operations in the field, ATS-Inbound and ATS-Outbound have proved to be effective means of identifying suspicious cargo that requires further investigation by CBP officers. The results of ATS-Inbound and ATS-Outbound analyses identifying cargo as suspicious have been regularly corroborated by physical searches of the identified cargo.

The goal of the Advanced Targeting Initiative is to enhance CBP officers' ability to identify entities such as organizations, cargo, vehicles, and conveyances with a possible association to terrorism. By their very nature, the results produced by technologies used in the Advanced Targeting Initiative may be only speculative or inferential; they may only provide leads for further investigation rather than a definitive statement. The program finds it valuable to be able to very quickly produce useful leads gleaned from masses of information. Leads resulting in a positive, factual determination obtained through further investigation and physical inspections of cargo demonstrate the efficacy of these technologies.

v. Laws and Regulations

There are numerous customs and related authorities authorizing the collection of data regarding the import and export of cargo as well as the entry and exit of conveyances.[33] Additionally, ATS-Outbound and ATS-Inbound support functions mandated by Title VII of Public Law 104-208 (1996 Omnibus Consolidated Appropriations Act for FY 1997), which provides funding for counter-terrorism and drug law enforcement. ATS-Outbound also supports functions arising

[32] ATS-Inbound collects information regarding individuals in connection with the following items including, but not limited to: Sea/Rail Manifests from AMS; Cargo Selectivity Entries and Entry Summaries from the Automated Broker Interface (ABI), a component of ACS; Air Manifests (bills of lading) from AMS; Express Consignment Services (bills of lading); CCRA Manifests (bills of lading from Canada Customs and Revenue (CCRA)); CBP Automated Forms Entry Systems (CAFES) CBP Form 7512; QP Manifest Inbound (bills of lading) from AMS; Truck Manifests from ACE; Inbound Data (bills of lading) from AMS; entries subject to Food and Drug Administration (FDA) Prior Notice (PN) requirements from ACS; and Census Import Data from the U.S. Department of Commerce.

[33] *See, e.g.*, 19 U.S.C. §§ 482, 1431, 1433, 1461, 1496, 1499, 1581-1583; 22 U.S.C § 401; and 46 U.S.C. § 46501.

from the Anti-Terrorism Act of 1987[34] and the 1996 Clinger-Cohen Act.[35] The risk assessments for cargo are also mandated under Section 203 of the SAFE Port Act.

b) ATS – Passenger Module

i. Program Description

ATS-P is a custom-designed system used at U.S. ports of entry, particularly those receiving international flights and voyages (both commercial and private), to evaluate passengers and crew members prior to arrival or departure. ATS-P facilitates the CBP officer's decision-making process about whether a passenger or crew member should receive additional screening prior to entry into, or departure from, the country because that person may pose a greater risk for terrorism and related crimes or other violations of U.S. law. ATS-P is a fully operational application that utilizes CBP's System Engineering Life Cycle methodology[36] and is subject to recurring systems maintenance. ATS-P is operational and has no set retirement date.

ii. Technology and Methodology

ATS-P processes traveler information against other information available to ATS, and applies threat-based scenarios comprised of risk-based rules, to assist CBP officers in identifying individuals who require additional inspection or in determining whether individuals should be allowed or denied entry into the United States. The risk-based rules are derived from discrete data elements, including criteria that pertain to specific operational or tactical objectives or local enforcement efforts. Unlike in the cargo environment, ATS-P does not use a score to determine an individual's risk level; instead, ATS-P compares information in ATS source databases against watch lists, criminal records, warrants, and patterns of suspicious activity identified through past investigations and intelligence. The results of these comparisons are either assessments of the threat-based scenario(s) that a traveler has matched, or matches against watch lists, criminal records and/or warrants. The scenarios are run against continuously updated incoming information about travelers (e.g., information in passenger and crew manifests) from the data sources listed below. While the risk-based rules are initially created based on information derived from past investigations and intelligence (rather than derived through data mining), data mining queries of data in ATS and its source databases may be subsequently used by analysts to refine or further focus those rules to improve the effectiveness of their application.

The results of queries in ATS-P are designed to signal to CBP officers that further inspection of a person may be warranted, even though an individual may not have been previously associated with a law enforcement action or otherwise noted as a person of concern to law enforcement. The risk assessment analysis is generally performed in advance of a traveler's arrival in or departure from the United States, and becomes one more tool available to DHS officers in determining a traveler's admissibility and in identifying illegal activity. In lieu of more

[34] 22 U.S.C. § 5201 *et. seq.*
[35] 40 U.S.C. § 1401 *et seq.*
[36] CBP's Office of Information & Technology's System Engineering Life Cycle (SELC) is a policy that lays out the documentation requirements for all CBP information technology projects, pilots, and prototypes. All projects and system changes must have disciplined engineering techniques, such as defined requirements, adequate documentation, quality assurance, and senior management approvals, before moving to the next stage of the life cycle. The SLC has seven stages: initiation and authorization, project definition, system design, construction, acceptance and readiness, operations, and retirement.

extensive manual reviews of traveler information and intensive interviews with every traveler arriving in or departing from the United States, ATS-P allows CBP personnel to focus their efforts on potentially high-risk passengers. CBP does not make unevaluated automated decisions about individuals based on the information in ATS-P. Rather, the CBP officer uses the information in ATS-P to assist in determining whether an individual should undergo additional inspection or should be allowed or denied entry into the United States.

iii. Data Sources

ATS-P uses available information from the following databases to assist in the development of the risk-based rules discussed above. ATS-P screening relies upon information in APIS; NIIS, which contains all Form I-94 Notice of Arrival/Departure records; ESTA, which in June 2010 replaced the I-94W document as the official form[37] and contains pre-arrival information for persons traveling from Visa Waiver Program (VWP)[38] countries (separately maintained in NIIS); the DHS Suspect and Violator Indices (SAVI); and the Department of State visa databases. ATS-P also relies upon PNR information from commercial airlines, TECS crossing data, seizure data, CMIR data, and information from the consolidated and integrated terrorist watchlist (Terrorist Watchlist) maintained by the TSC.

iv. Efficacy

ATS-P provides information to its users in near real time. The flexibility of ATS-P's design and cross-referencing of databases permits CBP personnel to employ information collected through multiple systems within a secure information technology system, to detect individuals requiring additional scrutiny. The automated nature of ATS-P greatly increases the efficiency and effectiveness of the officer's otherwise manual and labor-intensive work checking individual databases, and thereby helps facilitate the more efficient movement of travelers while safeguarding the border and the security of the United States. CBP officers use the information generated by ATS-P to aid their decision making about risk associated with individuals. As discussed below, ATS includes real-time updates of information from ATS source systems to ensure that CBP officers are acting upon accurate information.

In the past year, ATS-P has identified, through lookouts and/or scenario-based rule sets, individuals who were confirmed matches to the Terrorist Watchlist and prevented them from boarding an aircraft. ATS-P matches have enabled CBP officers and foreign law enforcement partners to disrupt and apprehend persons engaged in human trafficking and drug smuggling operations. For example, in one coordinated international effort from March through November of this year, there have been 82 identifications and interceptions of persons smuggling narcotics. In addition, ATS-P remains an effective tool in preventing child abductions involving individuals who are attempting to flee the United States in violation of a court order.

[37] Paper I-94Ws are still available at CBP ports of entry for use as a backup during system outages.

[38] The Visa Waiver Program allows eligible foreign nationals from participating countries to travel to the United States for business or pleasure, for stays of 90 days or less, without obtaining a visa. The Program requirements primarily are set forth in section 217 of the Immigration and Nationality Act, 8 U.S.C. § 1187, and 8 C.F.R. part 217. Section 711 of the 9/11 Commission Act amended section 217 to strengthen the security of the VWP. ESTA is an outgrowth of that mandate. More information about ESTA is *available at* http://www.cbp.gov/esta.

v. Laws and Regulations

CBP is responsible for collecting and reviewing information from travelers entering and departing from the United States.[39] As part of this inspection and examination process, each traveler seeking to enter the United States must first establish his or her identity, nationality, and, where appropriate, admissibility to the satisfaction of the CBP officer and must submit to inspection for customs purposes. The information collected is authorized pursuant to the Enhanced Border Security and Visa Reform Act of 2002,[40] ATSA, the Intelligence Reform and Terrorism Prevention Act of 2004,[41] Immigration and Nationality Act, as amended,[42] and the Tariff Act of 1930, as amended.[43] Much of the information collected in advance of arrival or departure can be found on routine travel documents that passengers and crew members may be required to present to a CBP officer upon arrival in or departure from the United States.

3. Privacy Impact and Privacy Protections

The Privacy Office has worked closely with CBP to ensure that ATS satisfies the privacy documentation required for operation. CBP completed a new PIA and published a SORN for all six ATS modules in August 2007.[44] Authorized CBP officers and personnel from ICE, TSA, and U.S. Citizenship and Immigration Services (USCIS) who are located at seaports, airports, land border ports, and operational centers around the world use ATS to support targeting, inspection, and enforcement related requirements.[45] ATS supports, but does not replace, the decision-making responsibility of CBP officers and analysts. Decisions or actions taken about individuals are not based solely upon the results of automated searches of data in the ATS system. The information obtained in such searches merely serves to assist CBP officers and analysts in either refining their analysis or formulating queries to obtain additional information upon which to base decisions or actions regarding individuals crossing U.S. borders.

ATS relies upon its source systems to ensure the accuracy and completeness of the data they provide to ATS. When a CBP officer identifies any discrepancy regarding the data, the officer will take action to correct that information, when appropriate. ATS monitors source systems for changes to the source system databases. Continuous source system updates occur in real time, or near real time, from TECS, which includes data from the National Crime Information Center (NCIC) as well as from ACE, AMS, ACS, AES, ESTA, NIIS, BCI, and APIS. When corrections are made to data in source systems, ATS updates this information immediately and uses only the

[39] *See, e.g.*, 19 U.S.C. §§ 482, 1431, 1433, 1461, 1496, 1499, 1581-1583; 8 U.S.C. §§ 1221, 1357; 22 U.S.C. § 401; 46 U.S.C. § 46501; and 49 U.S.C. § 44909.
[40] Pub. L. No. 107-173.
[41] Pub. L. No. 108-458.
[42] 8 U.S.C §§ 1185,1225.
[43] 19 U.S.C. §§ 66, 1433, 1454, 1485, 1624, and 2071.
[44] The PIA is *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats_updated_fr.pdf. The SORN is *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_sorn_cbp_ats_fromFR.pdf, and in the Federal Register at 72 Fed. Reg. 43,650 (Aug. 6, 2007). CBP published an update to the PIA in December 2008 to reflect new requirements regarding information pertaining to cargo to be submitted by importers and vessel carriers before the cargo is brought to the U.S. by vessel. The PIA update is *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_atsupdate10plus2.pdf.
[45] TSA, ICE, USCIS, and personnel from the DHS Office of Intelligence and Analysis (I&A) have access only to a limited version of ATS. I&A personnel use ATS in support of their authorized intelligence activities in accordance with applicable law, Executive Order, and policy.

latest data. In this way, ATS integrates all updated data (including accuracy updates) in as close to real time as possible.[46]

In the event that PII (such as certain data within a PNR) used by or maintained in ATS-P is believed by the data subject to be inaccurate, a redress process has been developed. The individual is provided information about this process during examination at secondary inspection. CBP officers have a brochure available to each individual entering and departing from the United States that provides CBP's Pledge to Travelers. This pledge gives each traveler an opportunity to speak with a passenger service representative to answer any questions about CBP procedures, requirements, policies, or complaints.[47] CBP has created a Customer Satisfaction Unit in its Office of Field Operations to provide redress with respect to inaccurate information collected or maintained by its electronic systems, including ATS. This process is available even though ATS does not form the sole basis for identifying enforcement targets. To facilitate the redress process, DHS has created a comprehensive, government-wide program, the Traveler Redress Inquiry Program (TRIP), to receive all traveler related comments, complaints, and redress requests affecting its component agencies. Through TRIP, a traveler can seek correction of erroneous PNR information stored in ATS and information stored in other DHS databases.[48]

Under the ATS SORN and as a matter of DHS policy, CBP permits any subject of PNR or his or her representative to make administrative requests for access and amendment of the PNR. Procedures for individuals to access ATS information are outlined in the ATS SORN and PIA. Individuals may gain access to their own data from source systems that provide input to ATS in accordance with the procedures set out in the SORN for each source system. The FOIA provides an additional means of access to PII held in source systems. Privacy Act and FOIA requests for access to information for which ATS is the source system are directed to CBP.[49]

ATS underwent the C&A process in accordance with DHS and CBP policy and obtained its initial C&A on June 16, 2006. ATS also completed a Security Risk Assessment on March 28, 2006, in compliance with FISMA, OMB policy, and National Institute of Standards and Technology guidance. The ATS C&A and Security Risk Assessment were subsequently updated and are valid until January 2011. The renewal process for the ATS C&A and Security Risk Assessment is currently underway.

Access to ATS is audited periodically to ensure that only appropriate individuals have access to the system. CBP's Office of Internal Affairs also conducts periodic reviews of ATS to ensure that the system is only being accessed and used in accordance with documented DHS and CBP

[46] To the extent information that is obtained from another government source is determined to be inaccurate, this problem would be communicated to the appropriate government source for remedial action.

[47] In addition, travelers can visit CBP's Customer Service web site *at* http://www.cbp.gov/xp/cgov/travel/customerservice/ to request answers to questions and submit complaints electronically. This website also provides travelers with the address of the Customer Service Center and the telephone number of the Joint Intake Center. Travelers may also file complaints through the DHS Traveler Redress Inquiry Program (DHS TRIP) by visiting the DHS TRIP website at http://www.dhs.gov/xtrvlsec/programs/gc_1169676919316.shtm.

[48] DHS TRIP can be accessed at: http://www.dhs.gov/files/programs/gc_1169676919316.shtm (*see,* 72 Fed. Reg. 2294, January 18, 2007).

[49] Requests may be submitted by mail to FOIA Division, 799 9th Street NW, Mint Annex, Washington, DC 20229-1177, by email to CBPFOIA@dhs.gov, or by phone to the CBP FOIA office is (202) 325-0150.

policies. Access to the data used in ATS is restricted to persons with a clearance approved by CBP, approved access to the separate local area network, and an approved password. All CBP process owners and all system users are required to complete annual training in privacy awareness and must pass an examination. If an individual does not take training, that individual loses access to all computer systems, which are integral to his or her duties as a CBP officer. Finally, as a condition precedent to obtaining access to ATS, CBP employees are required to meet all privacy and security training requirements necessary to obtain access to TECS.

As discussed above, ATS both collects information directly and derives other information from various systems. To the extent information is collected from other systems, data is retained in accordance with the record retention requirements of those systems.

The retention period for data maintained in ATS will not exceed fifteen years, after which time it will be deleted, except as noted below. The retention period for PNR, which is contained only in ATS-P, will be subject to the following further access restrictions: ATS-P users will have general access to PNR for seven years, after which time the PNR data will be moved to dormant, non-operational status. PNR data in dormant status will be retained for an additional eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security and only in response to an identifiable case, threat, or risk.

Notwithstanding the foregoing, information maintained only in ATS that is linked to law enforcement lookout records, CBP matches to enforcement activities, investigations or cases (i.e., specific and credible threats, and flights, individuals and routes of concern, or other defined sets of circumstances), will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

A National Archives and Records Administration (NARA) Electronic Records Appraisal Questionnaire was completed for PNR data in spring 2005. On April 12, 2008, NARA approved the record retention schedule for data retained in ATS.

B. Data Analysis and Research for Trade Transparency System (DARTTS)

1. 2010 Program Update

During the current reporting period, the ICE Office of Homeland Security Investigations (HSI)[50] transitioned DARTTS from a stand-alone system to the ICE enterprise network to expand DARTTS to a broader user base of ICE field agents, subject to appropriate access controls. The transition was initiated in April 2010, and ICE is continuing to deploy the enterprise version. ICE also implemented new auditing capabilities to enhance the overall integrity and accountability of DARTTS.

The 2009 DHS Data Mining Report[51] noted ICE's plans to add two data sources for DARTTS from the Department of the Treasury Financial Crimes Enforcement Network (FinCEN). The

[50] HSI, formerly known as the Office of Investigations, was established during ICE's internal re-organization in June 2010.

[51] 2009 DHS Data Mining Report at 13, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2009_12.pdf.

first is Suspicious Activity Reports filed by casinos, card clubs, and money services businesses.[52] The second is financial data provided in the Report of Foreign Bank and Financial Accounts (FBAR), which is filed by U.S. persons who have a financial interest in, or signature authority or other authority over any financial accounts in a foreign country, if the aggregate value of the accounts exceeds $10,000 at any time during the calendar year.[53] ICE has since incorporated these new data sources, and on April 26, 2010, ICE updated and published the DARTTS PIA to address these new sources and to describe the transition of DARTTS to the ICE enterprise network.

2. Program Description

ICE maintains DARTTS, which generates leads for and otherwise supports ICE investigations of trade-based money laundering, contraband smuggling, trade fraud, and other import-export crimes. DARTTS analyzes trade and financial data to identify statistically anomalous transactions that may warrant investigation. These anomalies are then independently confirmed and further investigated by experienced ICE investigators.

DARTTS is owned and operated by the ICE Trade Transparency Unit (TTU). Trade transparency is the concept of examining U.S. and foreign trade data to identify anomalies in patterns of trade. Such anomalies can indicate trade-based money laundering or other import-export crimes that ICE is responsible for investigating, such as contraband smuggling, trafficking of counterfeit goods, misclassification of goods, and the over- or under-valuation of goods to hide the proceeds of illegal activities. As part of the investigative process, ICE investigators and analysts must understand the relationships among importers, exporters, and the financing for a set of trade transactions, to determine which transactions are suspicious and warrant investigation. DARTTS is designed specifically to make this investigative process more efficient by automating the analysis and identification of anomalies for the investigator.

DARTTS allows ICE to perform research and analysis that is not available in any other system because of the data it contains and the level of detail at which the data can be analyzed.[54] DARTTS does not seek to predict future behavior or "profile" individuals or entities (i.e., identify individuals or entities that meet a certain pattern of behavior that has been pre-determined to be suspect). Instead, it identifies trade and financial transactions that are statistically anomalous based on user-specified queries. Investigators follow up on the anomalous transactions to determine if they are in fact suspicious and warrant further investigation. Investigators gather additional facts, verify the accuracy of the DARTTS data, and use their judgment and experience in making that determination. Not all anomalies lead to formal investigations.

DARTTS is currently used by ICE Special Agents and Criminal Research Specialists who work on TTU investigations at ICE Headquarters or in the ICE field and foreign attaché offices, as

[52] Money services businesses are required by the Bank Secrecy Act (BSA) to complete and submit Suspicious Activity Reports to FinCEN. 31 U.S.C. § 5318. They include money transmitters; issuers, redeemers and sellers of money orders and travelers' checks; and check cashers and currency exchangers.

[53] FinCEN administers the BSA, which requires depository institutions and other industries vulnerable to money laundering to take precautions against financial crime, including reporting financial transactions possibly indicative of money laundering. 31 U.S.C. §§ 5311-5330.

[54] For instance, DARTTS allows investigators to view totals for merchandise imports and then sort on any number of variables, such as country of origin, importer name, manufacturer name, or total value.

well as properly cleared support personnel. In April 2010, ICE initiated the transition of DARTTS to the ICE enterprise network, making DARTTS available to a greater number of ICE agents in the field, subject to appropriate access controls. ICE is continuing to deploy the enterprise version throughout ICE.

3. Technology and Methodology

DARTTS uses trade data collected by CBP, other federal agencies and foreign governments, and financial data collected by CBP and FinCEN. DARTTS data is primarily related to international commercial trade and financial transactions. ICE does not collect information directly from individuals or entities for inclusion in DARTTS. Instead, ICE receives data from the sources listed below via CD-ROM, external storage devices, or electronic data transfer and loads the data into DARTTS. DARTTS uses COTS software to analyze raw trade and financial data to identify anomalies and other suspicious transactions. The software application is designed for experienced investigators. It enables the analysis of structured and unstructured data using three tools: the drill-down technique,[55] link analysis, and charting and graphing tools that use proprietary statistical algorithms.[56] It also allows non-technical users with investigative experience to analyze large quantities of data and rapidly identify problem areas. The program makes it easier for investigators to apply their specific knowledge and expertise to complex sets of data.

DARTTS performs three main types of analysis. It conducts international trade discrepancy analysis by comparing U.S. and foreign import and export data to identify anomalies and discrepancies that warrant further investigation for potential fraud or other illegal activity. It performs unit price analysis by analyzing trade pricing data to identify over- or under-pricing of goods, which may be an indicator of trade-based money laundering. DARTTS also performs financial data analysis by analyzing financial reporting data (the import and export of currency, deposits of currency in financial institutions, reports of suspicious financial activities, and the identities of parties to these transactions) to identify patterns of activity that may indicate money laundering schemes.

DARTTS routinely receives bulk financial and trade information collected by other agencies and foreign governments,[57] hereafter referred to as "raw data." The sources of the raw data are described below. The agencies that provide DARTTS with trade data collect any PII directly from individuals or enterprises completing import-export electronic or paper forms.[58] The agencies that provide DARTTS with financial data receive PII from individuals and institutions,

[55] The drill-down system allows investigators to quickly find, analyze, share, and document suspicious patterns in large amounts of data, and to continually observe and analyze patterns in data at any point. Investigators can also connect from one dataset within DARTTS to another, to see whether the suspicious people, entities, or patterns occur elsewhere.

[56] DARTTS provides investigators the means to represent data graphically in graphs, charts, or tables to make identification of anomalous transactions easier and visually obvious. DARTTS does not create new records to be stored in DARTTS.

[57] Foreign trade data may include: names of importers, exporters, and brokers; addresses of importers and exporters; Importer IDs; Exporter IDs; Broker IDs; and Manufacturer IDs.

[58] U.S. trade data includes the following PII: names and addresses (home or business) of importers, exporters, brokers, and consignees; Importer and Exporter IDs (e.g., an individual's or entity's Social Security or Tax Identification Number); Broker IDs; and Manufacturer IDs.

such as banks, that are required to complete certain financial reporting forms.[59] The PII in the raw data is necessary to link related transactions together. It is also necessary to identify the persons or entities that should be investigated further.

ICE investigators with experience conducting financial, money laundering, and trade fraud investigations use the completed analysis to identify possible criminal activity and provide support to field investigators. TTU investigators at ICE Headquarters refer the results of DARTTS analyses to ICE field offices as part of an investigative referral package to initiate or support a criminal investigation. ICE investigators in the domestic field offices can also independently generate leads and subsequent investigations using DARTTS analysis. In addition, ICE investigators in attaché offices at U.S. embassies abroad have access to DARTTS on stand-alone terminals. These investigators use DARTTS to conduct analyses in support of financial, money laundering, and trade fraud investigations, and to respond to inquiries from partner-country TTUs with whom ICE shares anonymized U.S. trade data.

4. Data Sources

All of the raw data in DARTTS is provided by other U.S. agencies and foreign governments, and is divided into three broad categories: U.S. trade data, foreign trade data, and U.S. financial data. The U.S. trade data in DARTTS is (1) import data in the form of an extract from the ACS, which CBP collects from individuals and entities importing merchandise into the U.S. who complete CBP Form 7501 (Entry Summary) or provide electronic manifest information via ACS, (2) export data that CBP and the U.S. Department of Commerce collect from individuals and entities exporting commodities from the U.S. using Commerce Department Form 7525-V (Shipper's Export Declaration) or through AES,[60] and (3) publicly available aggregated U.S. export data (i.e., data that does not include PII) purchased by ICE from the U.S. Department of Commerce.[61] In the DARTTS enterprise version, ICE plans to incorporate a new data module with bill of lading data, which is data provided by carriers to confirm the receipt and transportation of on-boarded cargo to a specified destination. This information includes consignee name and address, shipper name and address, container number, carrier, and bill of lading. It is collected by CBP via the AMS, and is provided to ICE through CD-ROM, external storage devices, or electronic data transfers for uploading into DARTTS. ICE updated the DARTTS PIA to include the new bill of lading module.

The foreign import and export data in DARTTS is provided to ICE by partner countries pursuant to a Customs Mutual Assistance Agreement (CMAA) or other similar agreement. Certain countries provide trade data that has been stripped of PII. Other countries provide complete trade data, which includes any individuals' names and other identifying information that may be contained in the trade records.

[59] U.S. financial data includes the following PII: names of individuals engaging in financial transactions that are reportable under the BSA (e.g., cash transactions over $10,000); addresses; Social Security/Taxpayer Identification Numbers; passport number and country of issuance; bank account numbers; party names and addresses; and owner names and addresses.

[60] AES is operated jointly by the U.S. Census Bureau and CBP.

[61] This dataset is known as the U.S. Exports of Merchandise Dataset and is further described (including a complete list of data fields) on the U.S. Department of Commerce website *available at* http://www.census.gov/foreign-trade/reference/products/catalog/expDVD.html.

ICE receives U.S. financial data from FinCEN for uploading into DARTTS. This data is in the form of the following financial transaction reports: CMIRs (declarations of currency or monetary instruments in excess of $10,000 made by persons coming into or leaving the United States); Currency Transaction Reports (deposits or withdrawals of $10,000 or more in currency into or from depository institutions and casinos and card clubs); Suspicious Activity Reports (information regarding suspicious financial transactions within depository institutions, money services businesses, the securities and futures industry, and casinos and card clubs); Reports of Cash Payments over $10,000 Received in a Trade or Business (reports of merchandise purchased with $10,000 or more in currency); and FBAR data (reports of financial interest in foreign financial accounts in excess of $10,000).

DARTTS itself is the source of analyses of the raw data produced using COTS software analytical tools within the system. In addition, DARTTS creates extracts of U.S. trade data that has been stripped of PII, and provides those extracts to partner countries that operate their own TTUs and with whom the United States has entered into a CMAA or other similar agreement. The U.S. financial data in DARTTS is not shared with partner countries.

5. Efficacy

DARTTS has proved to be a useful tool for ICE in identifying criminal activity. To date, the ICE TTU has initiated several case referrals and continues to support ongoing investigations. Information from DARTTS has assisted in several criminal prosecutions. For example, using information gathered through DARTTS, ICE was able to disrupt a criminal organization involved in the illegal exportation of electronics to a U.S. designated terrorist entity in Paraguay. Three defendants were arrested in February 2010 for charges including violation of the International Emergency Economic Powers Act (IEEPA), smuggling electronic goods from the United States to Paraguay, and conspiracy. On October 20, 2010, all three defendants pled guilty to the export smuggling and conspiracy charges.

6. Laws and Regulations

ICE is authorized to conduct these law enforcement activities under 18 U.S.C. § 545 (Smuggling goods into the United States); 18 U.S.C. § 554 (Smuggling goods from the United States); 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 1956 (Laundering of Monetary Instruments); 19 U.S.C. § 1484 (Entry of Merchandise); and 50 U.S.C. §§ 1701-1706 (IEEPA), and DHS is authorized to maintain documentation of these activities pursuant to 19 U.S.C. § 2071 note (Cargo Information) and 44 U.S.C. § 3101 (Records Management by Agency Heads; General Duties). Information in DARTTS is regulated under the Privacy Act of 1974, the Trade Secrets Act,[62] and the Bank Secrecy Act.

7. Privacy Impact and Privacy Protections

ICE does not use DARTTS to make unevaluated automated decisions about individuals, and DARTTS data is never used directly as evidence to prosecute crimes. DARTTS is solely an analytical tool that helps in the identification of anomalies. It is incumbent upon the investigator who finds an anomaly to further investigate the reason for the anomaly. If the anomaly can be legitimately explained, the investigator has no need to further investigate it for criminal violations and moves on to the next identifiable anomaly. In addition, ICE investigators are

[62] 18 U.S.C. § 1905.

required to obtain and verify the original source data from the agency that collected the information, to prevent inaccurate information from propagating. All information obtained from DARTTS is independently verified before it is acted upon or included in an ICE investigative or analytical report. Investigators follow up on anomalous transactions to determine if they are in fact suspicious and warrant further investigation. They gather additional facts, verify the accuracy of the DARTTS data, and use their judgment and experience in making that determination.

DARTTS data is generally subject to access and amendment requests under the Privacy Act of 1974 and FOIA, unless a statutory exemption covering specific data applies. The U.S. and foreign government agencies that collect the information uploaded into DARTTS are responsible for providing appropriate notice on the forms used to collect the information, or through other forms of public notice, such as SORNs.[63] DARTTS will coordinate requests for access or to amend data with the original data owner. During the reporting year, ICE worked closely with the Privacy Office to complete and publish an updated PIA for DARTTS.[64]

As all of the information in DARTTS is obtained from other governmental organizations that collect the data under specific legislative authority, DARTTS cannot independently verify the accuracy of the data it receives. The owner of the source data is responsible for maintaining and checking the accuracy of its own data. In many instances, the data ultimately loaded into DARTTS is highly accurate because it is collected directly from the individual. In other instances, however, the data about individuals is provided to a governmental organization by a third party. In the event that errors are found, the DARTTS system owner must notify the agency that originally collected the data. FinCEN currently provides ICE with corrections to existing data, which are then uploaded into DARTTS. ICE does not, however, receive data corrections on trade data.

DARTTS re-completed its C&A and was granted a three year authority to operate (ATO) from DHS IT Security on April 22, 2010. In April 2010, DARTTS began its transition to the ICE enterprise network and is now maintained within the secure DHS network firewall. Any violations of system security or suspected criminal activity will be reported to the DHS Office of Inspector General, to the Office of the Information System Security Manager team in accordance with the DHS security standards, and to the ICE Office of Professional Responsibility.

All DARTTS users are assigned unique user IDs and passwords. Audit trails are used to track the date and time of login and sequences of users' actions and queries. New audit trail functionality has been implemented to provide an even more detailed trail and a higher level of integrity and accountability. The new audit trail features for the DARTTS enterprise version automatically track each action that occurs in the system, the date and time the action occurs, and which user performed the action. Only authorized personnel have access to audit trails, which

[63] The following SORNs are published in the Federal Register and describe the raw data ICE receives from U.S. agencies for use in DARTTS: for FinCEN Information, Suspicious Activity Report System (Treasury/FinCEN .002) and Bank Secrecy Act Reports System (Treasury/FinCEN .003); for Commerce Department Information, Individuals Identified in Export Transactions System (Commerce/ITA-1); and for CBP Information, Automated Commercial Environment/International Trade Data System (ACE/ITDS) (DHS/CBP-001).

[64] The PIA is available on the Privacy Office website at http://www.dhs.gov/privacy. DARTTS is covered by the SORN for the ICE Trade Transparency and Analysis Research (TTAR) system of records. The SORN is available on the Privacy Office website at http://www.dhs.gov/privacy and in the Federal Register at 74 FR 39083 (August 5, 2009).

are kept for a minimum of 90 days. Audit trails are reviewed by DARTTS system administrators or the Information System Security Officer. The system administrator also maintains a spreadsheet record of the receipt or distribution of sensitive information on electronic media.[65]

Access to DARTTS is granted on a case-by-case basis by the TTU Network Administrator. Access is currently limited to ICE users working on TTU investigations, as well as properly cleared support personnel. All individuals who are granted system use privileges are properly cleared to access the information within DARTTS.

In 2009, NARA approved a record retention period for the information maintained in DARTTS. ICE maintains the records in DARTTS for five years and then archives the records for five additional years, for a total retention period of 10 years. The five-year retention period for records is necessary to create a data set large enough to effectively identify anomalies and patterns of behavior in trade transactions. Records older than five years will be removed from the system and archived for five additional years and will only be used to provide a historical basis for anomalies in current trade activity. The original CD-ROMs containing the raw data will be retained for five years to ensure data integrity and for system maintenance.

C. Freight Assessment System (FAS)

1. 2010 Program Update

FAS is now being used to analyze screening data from domestic Air Carriers, Indirect Air Carriers who are certified to screen cargo, Certified Shippers, and Independent Screening Facilities. This functionality within FAS is called the Cargo Report Tool (CRT). As reported in the 2009 DHS Data Mining Report, FAS data mining capabilities have not yet been deployed.

2. Program Description

The TSA FAS is a risk-assessment tool that can be used to identify cargo that may pose a heightened risk to passenger aircraft. FAS was originally designed to reduce the reliance on random inspections conducted by industry. FAS uses a rules-based model developed by security subject-matter experts. The model is software-based and incorporates machine-derived rules and predictive indicators to identify and assess high-risk cargo. Once FAS is fully operational, cargo identified as high-risk will be flagged and set aside for further inspection by air carriers. The system will also provide this information to TSA cargo inspectors or canine teams. FAS neither uses nor stores PII.

FAS was originally designed to support the mandates of the 2003 TSA Air Cargo Strategic Plan. Section 1602 of the 9/11 Commission Act, which was enacted during the FAS design and development process, added new requirements relating to the percentage of cargo to be screened to the Air Cargo strategic goals and mission. The FAS will be another layer of security to identify domestic cargo for secondary screening and could be used to assess risk for international inbound cargo as well. FAS facilitates government-managed, risk-based assessments of cargo

[65] DARTTS receives CD-ROMs and other external storage media provided by other agencies. Once data from CD-ROMs or other external storage media is loaded onto DARTTS, the TTU Network Administrator stores them in the secured server room located in the TTU offices at ICE Headquarters until the retention period has elapsed, at which point they are destroyed.

and chain-of-custody oversight throughout the supply chain, including locations far from the air carrier where the risk is more significant.

With help from selected industry participants in the air cargo supply chain, FAS completed pre-system testing. The results indicated that implementing FAS in participants' business operations had only a minor impact on the efficiency of those operations. FAS re-certified its C&A from DHS/TSA IT Security on May 23, 2010 and received its ATO for two additional years. FAS's development stage is now concluded, and FAS is being used to receive and analyze cargo handled by Air Carriers, Certified Independent Screening Facilities, Certified Shippers, and Indirect Air Carriers who have joined the Certified Screening Program. This reporting capability is part of FAS's software suite functionality. FAS data mining capabilities are not yet operational, but will be used when FAS is fully deployed. The planned FAS life cycle is 10 years.

3. Technology and Methodology

FAS uses COTS software to collect, fuse, and analyze data related to supply chain, logistics, and freight transportation data. The software serves as the information platform that supports TSA's layered security approach. It (1) applies risk-based analytical rules to the supply chain data to assist analysts in scrutinizing cargo as it is being screened, (2) provides an informational backbone that supports chain-of-custody integrity, and (3) assists management in determining the optimal usage of inspection resources. The software includes a rules-management platform that enables the application of business process, security, and data cleansing rules to each shipment. It also includes a process for incorporating information from screeners and analysts, based upon their real-world experience, into the risk-based rules development process.

4. Data Sources

FAS uses the air carriers' house and master airway bills (no PII from airway bills is included in the system), and data from the following TSA systems: the Performance and Results Information System (compliance data);[66] the Indirect Air Carrier Management System (IACMS) (TSA-assigned certification number);[67] and the Known Shipper Management System (KSMS) (company names).[68] FAS compares information in these TSA systems with company background information that it obtains from Dun & Bradstreet, and with publicly-available statistical data on criminal activity.

[66] PARIS compiles the results of cargo inspections and the actions taken when violations are identified. The PARIS database provides TSA a web-based method for entering, storing, and retrieving performance activities and information on TSA-regulated entities, including air carriers and indirect air carriers. PARIS includes profiles for each entity, inspections conducted by TSA, incidents that occur throughout the nation, such as instances of bomb threats, and investigations that are prompted by incidents or inspection findings.

[67] IACMS is a management system used by TSA to approve and validate new and existing Indirect Air Carriers. This management system and application is intended for freight forwarders wishing to receive TSA approval to tender cargo utilizing an Indirect Air Carrier certification. The IACMS is not intended for individuals wanting to ship cargo. An Indirect Air Carrier means any person or entity within the United States not in possession of a Federal Aviation Administration air carrier operating certificate that undertakes to engage indirectly in air transportation of property and uses, for all or any part of such transportation, the services of a passenger air carrier. *See* PIA on TSA's Air Cargo Security Requirements, which provides additional information on the privacy impact of the IACMS and KSMS. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_aircargo.pdf.

[68] KSMS uses commercial databases to verify the legitimacy of shippers. Known shippers are entities that have routine business dealings with freight forwarders or air carriers and are considered vetted shippers. In contrast, unknown shippers are entities that have conducted limited or no prior business with a freight forwarder or air carrier.

5. Efficacy

The software used in FAS has proven in various testing and operational deployments to be highly effective in providing accurate information in real time that supports TSA risk analysts (the primary users of the system) in their work. The value of the output generated by the software will be determined by the quality of the data inputs, including airway bills, the primary document used in FAS. Where necessary, FAS can use the software's industry-specific capabilities (supply chain, logistics, and freight transportation) to enable data cleansing and the interpretation and improvement of any data that appears to be of lesser quality.

Validity testing was completed in a proof-of-concept that scored live airway bills with a prototype model of FAS. TSA found the results to be consistent with expectations and with CBP's ATS determinations. TSA was able to inspect cargo that the tools identified as presenting an elevated risk, and physical inspection confirmed the higher risk determination. Standards for validating the data mining models are included in the software used by FAS. The results of the FAS testing phase corroborate the results of the proof-of-concept validity testing.

6. Laws and Regulations

The legal and policy foundation for FAS is based in the ATSA, which established TSA and gave it responsibility for security in all modes of transportation;[69] the DHS/TSA Air Cargo Strategic Plan (November 2003), which sets forth TSA's commitment to work closely with federal, state, local, and industry partners to ensure that 100 percent of cargo that is deemed to be of elevated risk is inspected and that 100 percent of the cargo supply chain is secure; and Section 1602 of the 9/11 Commission Act, which requires TSA to provide a level of security for cargo on commercial flights that is commensurate with the level of security provided for passenger checked baggage. The 9/11 Commission Act also sets the inspection benchmarks of 50% of cargo screened not later than 18 months after the date of enactment, and 100% of cargo screened not later than three years after date of enactment.

7. Privacy Impact and Privacy Protections

FAS submitted a PTA to the DHS Privacy Office. As TSA specifically designed FAS not to hold any PII, individual privacy is not affected by FAS and no privacy documentation beyond the PTA is required. Dun & Bradstreet data is used to confirm that the Indirect Air Carrier certification issued to a business owner matches the name on the certificate issued by TSA's Indirect Air Carrier regional coordinators. The information regarding the business owner is not entered into FAS as a factor and is not stored. It is used only to verify the name of the business owner.

FAS obtained its C&A from DHS/TSA IT Security, demonstrating its full compliance with DHS information technology security requirements. Access to FAS is limited to authorized users. Unauthorized access is controlled through system lockdowns, role-based access control, and the use of authentication servers. HTTPS will be the only acceptable method of communication with the web server. Audit capability exists within FAS and will be used to review the reasons for system hits.

[69] Pub. L. No. 107-71 (2001).

FAS is being prioritized for operational implementation. FAS implementation plans call for retention of data in FAS for a period of 90 days for examination and analysis, after which the data will be archived for seven years.

III. Conclusion

The DHS Privacy Office is pleased to provide the Congress its fifth comprehensive report on DHS data mining activities. The Congress has authorized the Department to engage in data mining in furtherance of the DHS mission. The DHS Privacy Office has reviewed the programs described in this report, using the compliance documentation process it requires for DHS programs and systems generally to ensure that necessary privacy protections have been implemented. Each program has completed a PTA with the DHS Privacy Office's guidance, and programs that use PII have published PIAs and SORNS approved by the DHS Chief Privacy Officer. The DHS Privacy Office remains vigilant in its oversight of all Department programs and systems, including those that involve data mining.

IV. Appendices

A. Federal Agency Data Mining Reporting Act Reporting Requirements

The Act requires the Department to provide the Congress the following information about each program or activity that meets the Act's definition of "data mining:"

> *A thorough description of the data mining activity, its goals, and, where appropriate, the target dates for the deployment of the data mining activity.*
>
> *A thorough description of the data mining technology that is being used or will be used, including the basis for determining whether a particular pattern or anomaly is indicative of terrorist or criminal activity.*
>
> *A thorough description of the data sources that are being or will be used.*
>
> *An assessment of the efficacy or likely efficacy of the data mining activity in providing accurate information consistent with and valuable to the stated goals and plans for the use or development of the data mining activity.*
>
> *An assessment of the impact or likely impact of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.*
>
> *A list and analysis of the laws and regulations that govern the information being or to be collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity.*
>
> *A thorough discussion of the policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to protect the privacy and due process rights of individuals, such as redress procedures, and ensure that only accurate and complete information is collected, reviewed, gathered, analyzed, or used, and guard against any harmful consequences of potential inaccuracies.*[70]

The Privacy Office addresses these reporting requirements for each of the DHS programs included in this report.

[70] 42 U.S.C. § 2000ee-3(c)(2).

B. Acronym List

Acronym List	
ACE	Automated Commercial Environment
ACS	Automated Commercial System
ACSTP	TSA Air Cargo Division's Air Cargo Screening Technology Pilot
AES	Automated Export System
AMS	Automated Manifest System
APIS	Advance Passenger Information System
ATO	Authority to Operate
ATS	Automated Targeting System
ATSA	Aviation and Transportation Security Act
ATS-P	ATS Passenger Module
BCI	Border Crossing Information
BSA	Bank Secrecy Act
C&A	Certification and Accreditation
CBP	United States Customs and Border Protection
CMAA	Customs Mutual Assistance Agreement
CMIR	The Report of International Transportation of Currency or Monetary Instruments Form
COTS	Commercial Off-The-Shelf
CRT	Cargo Report Tool
CSI	Container Security Initiative
DARTTS	Data Analysis and Research for Trade Transparency System
DHS	Department of Homeland Security
EEI	Electronic Export Information
ESTA	Electronic System for Travel Authorization
FAS	Freight Assessment System
FBAR	Report of Foreign Bank and Financial Accounts
FBI	Federal Bureau of Investigation
FinCEN	Department of the Treasury Financial Crimes Enforcement Network
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
HSI	ICE Homeland Security Investigations Directorate
I&A	Office of Intelligence and Analysis
IACMS	Indirect Air Carrier Management System
ICE	Immigration and Customs Enforcement
IOFS	Intelligence and Operations Framework System
KSMS	Known Shipper Management System
NARA	National Archives and Records Administration
NCIC	National Crime Information Center
NIIS	Nonimmigrant Information System
PIA	Privacy Impact Assessment

Acronym List	
PII	Personally Identifiable Information
PNR	Passenger Name Record
PPOC	Privacy Point of Contact
PTA	Privacy Threshold Analysis
SAVI	Suspect and Violator Indices
SED	Shippers' Export Declaration
SELC	System Engineering Life Cycle
SFI	Secure Freight Initiative
SORN	System of Records Notice
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TTU	ICE Office of Investigations Trade Transparency Unit
USCIS	United States Citizenship and Immigration Services
VWP	Visa Waiver Program